

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Michael G. Gerfin, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent (SA) with the Federal Bureau of Investigation (“FBI”) for over nine years. During this time, I have been assigned to numerous investigations involving complex computer crimes. I am currently assigned to the FBI Cleveland Division Cyber Crimes Squad and am responsible for investigations involving computer-related offenses. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information. In addition to my work experience, I have received extensive specialized training in the field of computer crime investigation from the FBI and others. In addition to my investigative experience, I possess degrees in Computer Science and Physics and have been involved in the field of information technology for over 20 years. My previous employment consisted of roles in computer network administration and software engineering, and I hold numerous professional certifications in the field of computer security. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

1. This investigation pertains to the theft of over \$106,000 from Fifth Third Bank (“FIFTH THIRD”) ATMs in Illinois, Michigan, and Ohio. FIFTH THIRD is a federally insured financial institution that is headquartered in Cincinnati, Ohio, which is in the Southern District of Ohio.

2. This affidavit is intended to show only that there is sufficient probable cause for the requested Complaint and Arrest Warrant and does not set forth all of my knowledge about this matter.

PERTINENT FEDERAL CRIMINAL STATUTES

3. 18 USC 1343 – Wire Fraud

PROBABLE CAUSE

4. The information in this affidavit comes from my review of investigative reports, discussions with other law enforcement officers and witnesses, and personal observations and interactions. As such, I have subsequently learned the following information:

- a. In May 2018, FIFTH THIRD detected fraudulent activity originating from their mobile banking feature known as “cardless ATM”. Cardless ATM allows customers to withdraw money from a FIFTH THIRD ATM using only their mobile device and the FIFTH THIRD mobile banking application. Customers are not currently able to use this feature at another bank’s ATM. This eliminates the need for a physical card to withdraw cash from a FIFTH THIRD ATM.
- b. Upon further investigation, FIFTH THIRD found that an unknown actor had compromised the usernames and passwords, one-time passcodes, and PIN numbers for approximately 125 of their customers. A significant percentage of these customers reside in Cincinnati and the surrounding areas.
- c. Based on conversations FIFTH THIRD employees had with affected customers, FIFTH THIRD discovered that affected customers received phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led customers to a website that

mimicked the legitimate FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.

- d. After compromising the customer accounts, the unknown actor successfully cashed out approximately \$68,000 in total from 17 ATMs in Illinois, Michigan, and Ohio in less than two weeks through the cardless ATM function. FIFTH THIRD obtained photographic images from those ATM locations. At each location, the unknown actor was wearing a hat and sunglasses to disguise his identity.
- e. On or about October 3, 2018, FIFTH THIRD started to receive complaints that customers were receiving phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led customers to a website that mimicked the legitimate FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.
- f. On or about October 10, 2018, FIFTH THIRD detected fraudulent activity originating from their cardless ATM function. FIFTH THIRD identified two individuals (“Individual-1” and “Individual-2”) conducting the fraudulent activity at ATM locations in the Cincinnati metropolitan area.
- g. On or about October 15, 2018, FIFTH THIRD started to receive additional complaints that customers were receiving phishing messages via text message indicating that their accounts were locked. The text messages contained a link to unlock their accounts and led customers to a website that mimicked the legitimate

FIFTH THIRD website. The website required customers to enter the account credentials in order to unlock their accounts.

- h. On or about October 17, 2018, FIFTH THIRD detected additional fraudulent activity originating from their cardless ATM function. FIFTH THIRD identified a third individual (“Individual-3”) conducting the activity at an ATM on West Market Street in Fairlawn, Ohio, which is in the Northern District of Ohio.

FIFTH THIRD obtained photographic images from the ATM camera of Individual-3 with blonde facial hair wearing a hat and holding a phone.

5. On or about October 10, 2018, law enforcement located and arrested Individual-1 and Individual-2 in Cincinnati, Ohio. The investigation has since has shown connections between Individual-1 and Individual-2, as well as their connections to other, including yet unknown, co-conspirators.

6. On or about October 17, 2018, law enforcement located an individual matching the physical description of Individual-3 near the ATM on West Market Street in Fairlawn, Ohio. Fairlawn Police Department (“FPD”) arrested Individual-3 and identified him as ISTVAN LUKACS.

7. Records from FIFTH THIRD show that LUKACS attempted at least \$2,260 in ATM transactions and successfully withdrew \$800.00 from two FIFTH THIRD ATM locations.

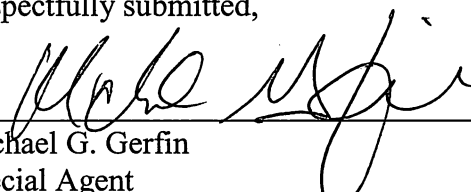
8. On October 18, 2018, LUKACS was taken into federal custody at the Summit County Jail, and indicated his name was ISTVAN LUKACS. Jail property included a Hungarian Passport in the name of ISTVAN LUKACS, with a date of birth of September 17, 1986. LUKACS additionally had advised arresting authorities that his date of birth was September 17, 1986.

9. On October 22, 2018, law enforcement personnel from Immigration and Customs Enforcement (ICE) informed the FBI that obtained finger print cards from arresting agency FPD revealed a true identity for LUKACS of JANOS MADARASZ, date of birth October 25, 1989. Official records also showed that MADARASZ a.k.a. LUCKACS has an Interpol warrant on charges of fraudulent travel documents.

CONCLUSION

10. Based on the foregoing, I believe that there is probable cause to show that JANOS MADARASZ has violated the aforementioned pertinent statutes.

Respectfully submitted,



Michael G. Gerfin
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 25, 2018



THE HONORABLE KATHLEEN B. BURKE
UNITED STATES MAGISTRATE JUDGE